IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

WATT

Appl. No. 10/714,481

Filed: November 17, 2003

Atty. Ref.: 550-481; Confirmation No. 8029

TC/A.U. 2189

Examiner: Flournoy, Horace L.

For: APPARATUS AND METHOD FOR CONTROLLING ACCESS TO A MEMORY UNIT

* * * * * * * * * * * *

August 15, 2006

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

STATEMENT OF ARGUMENTS IN SUPPORT OF PRE-APPEAL BRIEF REQUEST FOR REVIEW

The Examiner finally rejects all claims 1-20 under 35 U.S.C. §102(e) for anticipation based upon US-A-2003/0101322 (Gardner). To establish that a claim is anticipated, the Examiner must point out where each and every limitation in the claim is found in a single prior art reference. If even one limitation is missing from the reference, then it does not anticipate the claim. *Kloster Speedsteel AB v. Crucible, Inc.*, 793 F.2d 1565 (Fed. Cir. 1986). Gardner is missing several features from the independent claims.

Gardner describes a mechanism for protecting user application data so that it can be kept secret from root and other users (see Figure 6 and the associated description in paragraphs 0189 to 0193). There are four privilege levels PLO to PL3: PL0 is the most privileged level of the processor, and PL3 is the least privileged level. The operating system runs at privilege level PL2, and user applications run at privilege level PL3 (see paragraph 0019). Paragraph 0189 and Figure 6 describe how a user application operating at the least privileged level can keep its data secure from other users. Gardner refers to such user applications that require their data to be

kept secure as "secure user applications." To accomplish that security, Gardner uses protection keys which allow a secure user application "to access a page of memory in memory 74 that nobody else can access, including root or anything running at PL2 or above" (see paragraph 0190). The protection keys are inserted into protection key registers by code executing at the protection level PLO (paragraph 0191).

Error #1: Gardner's ELF User Process Security Bit Is Not a Bit Associated With Each Entry in the Memory Unit.

Claim 1 recites a memory unit that includes "a *flag being associated with each entry in the memory unit* to store a value indicating whether the one or more data items stored in the associated entry are said secure data or said non-secure data." The Examiner reads this claim feature onto Gardner's ELF header, citing paragraph 0189. An ELF header describes the layout of an executable file, and contains information such as the start address of the program code and the type of the code. Hence, each ELF header describes information about a particular piece of program code. As paragraph 0189 explains, secure user *processes* are distinguished from non-secure user *processes* by setting a bit in the ELF header. But distinguishing processes or program code is not what is claimed. Rather, the claimed flag is associated with *each entry in the memory unit.*

Gardner's ELF header does not teach associating a flag with each entry in the memory unit. Nor does Gardner disclose some other mechanism for marking individual entries in the memory unit as containing secure data or non-secure data to allow the memory unit to police memory unit accesses. Indeed, Gardner does not describe any details as to how data is stored with a memory unit. Consequently, Gardner does not prevent an access to a memory unit entry storing secure data from a non-secure domain.

Error #2: Gardner's Memory Unit Does Not Prevent Access From A Non-Secure Domain To Data In An Memory Entry Marked As Storing Secure Data.

Claim 1 further recites: "wherein when the processor is operating in said at least one non-secure mode of the non-secure domain, the memory unit is operable, upon receipt of a memory access request issued by the processor when access to an item of data is required, to prevent access to any data item within an entry of the memory unit that the associated flag indicates has secure data stored therein." The Examiner points again to Gardner's paragraph 0189: "in one embodiment, the information for distinguishing between secure and non-secure user processes is contained in a secure memory page in memory 74 that cannot be modified by PL2 code." This means that operating system level code cannot tamper with the information that distinguishes between secure and non-secure user processes, thereby alleviating the risk that a non-secure user process can be viewed as being secure via manipulation of that information stored in the secure memory page. But this has nothing to do with the claimed access of data in memory.

That Gardner safeguards the information for distinguishing between secure and non-secure user processes so that it cannot be modified by PL2 code is not relevant to claim 1. Claim 1 is not concerned with how to manage the issue of a non-secure application or process seeking to disguise itself as a secure application or process. Instead, claim 1 marks *data* stored in the memory unit on an entry-by-entry basis to identify the data in each entry as being either secure data or non-secure data. As a result of that data entry marking, the memory unit prevents access from a non-secure domain to any memory entry storing secure data.

Error #3: Gardner Does Not Perform The Allocation Of Individual Data As Either Secure Or Non-Secure Data In The Secure Domain.

The memory unit in claim 1 recites: "the allocation of data as either secure or non-secure data being performed in the secure domain." The Examiner's final action does not address this claimed feature, and it is not found in Gardner.

Error #4: Page Tables 140 And 142 Are Not The Claimed Plural Entries In Memory.

Claim 1 recites: "a memory unit comprising a plurality of entries and operable to store data required by the processor, each entry being operable to store one or more data items including either secure data or non-secure data." The Examiner refers to the page table 140 and the virtual hash page table (VHPT) 142 in Figure 3 of Gardner as the claimed "plurality of entries." The page table 140 is a structure used to map virtual memory pages to physical memory pages. That mapping structure itself is not secure or non-secure data (see paragraph 0047). The virtual hash page table (VHPT) is referred to when installing translation entries into the TLB 128 (see paragraph 0057). In contrast, claim 1 recites that the memory unit entries store secure or non-secure data. Neither the page table 140 nor the virtual hash page table 142 store any secure or non-secure data.

Error #5: Gardner Fails To Teach The Claimed Secure And Non-Secure Domains.

The Examiner refers to paragraph 0189 of Gardner as teaching secure and non-secure domains. In fact, that paragraph does not mention domains at all. Instead, paragraph 0189 merely refers to secure user applications and non-secure user applications, both of which are user applications running at the lowest privilege level PL3. Claim 1 employs three different terms: modes, programs, and domains. The processor can operate in a number of different modes of operation, for example a user mode, a supervisor mode, etc. In a particular mode of operation, the processor can execute programs. For example, a user application or program will typically be executed in a user mode of operation. But in addition to modes of operation and execution of programs, the processor can operate in a plurality of domains including a secure domain and a non-secure domain. As defined in claim 1, access to data is performed on a domain basis to ensure that data pertaining to the secure domain is not accessed from the non-secure domain.

From Figure 1 in Gardner, the different privilege levels might be equated with different modes of operation. But there is no disclosure of a separate and distinct classification which could reasonably be equated with the additionally claimed plurality of domains.

Given these multiple clear errors—any one of which defeats the anticipation rejection based on Gardner, the final rejection should be withdrawn and the application passed to allowance.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: _____
John R. Lastova
Reg. No. 33,149

JRL:maa
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100